DE 3927270

2/9/1
DIALOG(R)File 351:Derwent WPI

0005465471 - Drawing available
WPI ACC NO: 1991-066143/199110 XRPX Acc No: N1991-051165

Personalisation of coded data cards - providing cards with pseudo name which is overwrite with name when used

Patent Assignee: DEUT BUNDESPOST (DEBP); DEUT TELEKOM AG (DEBP)
Inventor: KOWALSKI B; WOLFENSTER K D; WOLFENSTETTER K

Patent Family (2 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
DE 3927270	A	19910228	DE 3927270	A	19890818	199110 B
DE 3927270	C2	19960711	DE 3927270	A	19890818	199632 E

Priority Applications (no., kind, date): DE 3927270 A 19890818

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
DE 3927270	C2	DE	7	4	

Alerting Abstract DE A

A system is used for the personalisation of data cards of the type used for access to banking services. The initial issue of the card is made with an individual code number (K) and a pseudo identify name (X) that is entered into a register (3). The values are entered on the card (2) and are read when the card is used for the first time.

When the transaction is made the user enters his time identify, which is then used to overwrite the pseudo identify in the register.

ADVANTAGE - Provides ease of personalising data cards. @(7pp Dwg.No.2/4)@

Title Terms /Index Terms/Additional Words: CODE; DATA; CARD; PSEUDO; NAME

Class Codes
International Classification (Main): G06K-019/073
(Additional/Secondary): G06K-019/10, G07C-009/00

File Segment: EPI;
DWPI Class: T05
Manual Codes (EPI/S-X): T05-D

Original Publication Data by Authority

Germany
Publication No. DE 3927270 A (Update 199110 B)
Publication Date: 19910228
Verfahren zum Personalisieren von Chipkarten
Assignee: Deutsche Bundespost, vertreten durch den Praesidenten des Fernmeldetechnischen Zentralamtes, 6100 Darmstadt, DE (DEBP)
Inventor: WOLFENSTER K D
Kowalski, Bernd, Dipl.-Ing., 5900 Siegen, DE
Language: DE
Application: DE 3927270 A 19890818 (Local application)
Original IPC: G07C-9/00
Current IPC: G07C-9/00
Claim:
* 1. Verfahren zum Personalisieren von Chipkarten bei dem der Name des

Teilnehmers und ein zugehoriger individueller Schlussel in die Chipkarte abgespeichert werden und der Name des Teilnehmers in ein Register abgelegt wird,
dadurch gekennzeichnet, dass in einem gesicherten Bereich (**1**) die Chipkarte (**2**) statt mit dem Namen des Teilnehmers (A) mit einer Pseudo- Indentitat (X) vorpersonalisiert wird und diese Pseudo- Indentitat (X) in dem Register (**3**) abgelegt wird und dass erst nach Verlassen der Chipkarte (**2**) des gesicherten Bereichs (**1**) in einer Kartenausgabestelle zur Selbstpersonalisierung die Pseudo-Identitat (X) mit dem Namen des Teilnehmers (A) uberschrieben wird und dass dieser Name uber eine gesicherte Kommunikationsverbindung zum gesicherten Bereich (**1**) der Pseudo-Identitat im Register (**3**) fest zugeordnet wird.

Publication No. DE 3927270 C2 (Update 199632 E)
Publication Date: 19960711
Verfahren zum Personalisieren von Chipkarten
Assignee: Deutsche Telekom AG, 53113 Bonn, DE (DEBP)
Inventor: Wolfenstetter, Klaus-Dieter, Dipl.-Math., 6146 Alsbach, DE
Kowalski, Bernd, Dipl.-Ing., 5900 Siegen, DE
Language: DE (7 pages, 4 drawings)
Application: DE 3927270 A 19890818 (Local application)
Original IPC: G06K-19/073(A) G06K-19/10(B)
Current IPC: G06K-19/073(A) G06K-19/10(B)
Claim:
* 1. Verfahren zum Personalisieren von Chipkarten (**2**), bei dem ein Teilnehmername (A) und ein individueller Schlussel (K) in die Chipkarten (**2**) abgespeichert werden und der Teilnehmername in einem gesicherten Bereich (**1**) in einem Register (**3**) abgelegt und die Chipkarten danach ausgeliefert werden, **dadurch gekennzeichnet,**
* - dass im gesicherten Bereich (**1**) anstelle des Teilnehmernamens (A) ein Pseudoname (X) in die Chipkarte eingetragen wird,
* - dass in einer Kartenausgabestelle (**5**) vor der Kartenausgabe der Pseudoname (X) in der Chipkarte (**2**) mit dem Teilnehmernamen (A) uberschrieben wird,
* - dass uber eine gegen Abhoren und Verandern von zu ubertragenden Daten gesicherte Kommunikationsverbindung (**6**) zwischen der Kartenausgabestelle (**5**) und dem gesicherten Bereich (**1**) der Pseudoname (X) und der Teilnehmername (A) verschlusselt zum gesicherten Bereich (**1**) ubertragen werden,
* - dass in einem Register (**3**) des gesicherten Bereiches (**1**) der Teilnehmername (A) zum Pseudonamen (X) zugeordnet gespeichert wird, und
* - dass nach einer Ruckmeldung vom gesicherten Bereich (**1**) zur Kartenausgabestelle (**5**) dort die Ausgabe der personalisierten Chipkarte (**2**) erfolgt.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3927270 A1**

(51) Int. Cl. 5: G07C 9/00

(21) Aktenzeichen: P 39 27 270.2
(22) Anmeldetag: 18. 8. 89
(43) Offenlegungstag: 28. 2. 91

DE 3927270 A1

(71) Anmelder:

Deutsche Bundespost, vertreten durch den Präsidenten des Fernmeldetechnischen Zentralamtes, 6100 Darmstadt, DE

(72) Erfinder:

Wolfenstetter, Klaus-Dieter, Dipl.-Math., 6146 Alsbach, DE; Kowalski, Bernd, Dipl.-Ing., 5900 Siegen, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Personalisieren von Chipkarten

Bisher wurden Chipkarten nur innerhalb eines gesicherten Bereichs zentral personalisiert. Die durch den Versand der Karten aufkommenden Wartezeiten für die Kunden sollen durch die Erfindung vermieden werden.
Gemäß der Erfindung werden die Chipkarten (2) in dem gesicherten Bereich (1) mit einer Pseudoidentität (x) vorpersonalisiert und nach Bedarf erst in den Kartenausgabestellen mit dem Namen des Teilnehmers (A) versehen (endpersonalisiert). Die Endpersonalisierung wird von einer berechtigten Person durchgeführt und die Daten dem gesicherten Bereich über eine gesicherte Kommunikationsverbindung mitgeteilt. Diese Personalisierungsprozedur ist bei allen Chipkartenanwendungsbereichen verwendbar.

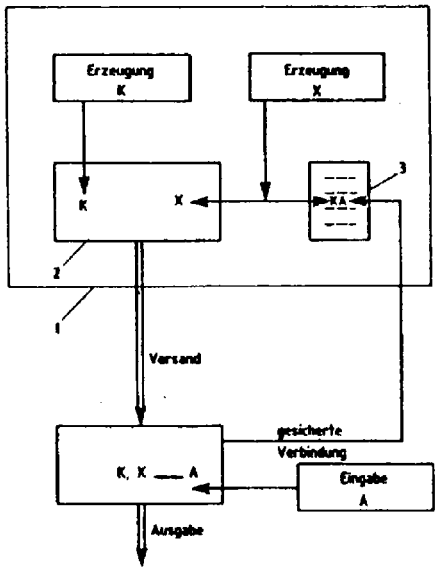

Fig. 2

DE 3927270 A1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Personalisieren von Chipkarten.

Es ist aus der Zeitschrift Telecom report 12 (1989), Heft 1–2, S. 56 bis 58 bereits ein Stand der Technik bekannt, gemäß dem die Personalisierung von Chipkarten zentral in einer gesicherten Umgebung erfolgt. Bei diesem Vorgang werden bereits die endgültigen Personalisierungsdaten in den Chip der Karte eingeschrieben.

Die Freigabe der Chipkarte erfolgt später durch Eingabe der persönlichen Identifikationsnummer (PIN) durch den Benutzer.

Nachteilig bei diesem Stand der Technik ist, daß bereits beim zentralen Personalisieren die vollständigen Daten des späteren Benutzers vorliegen müssen.

Aufgabe der Erfindung ist es, den Personalisierungsvorgang dezentral durchführen zu können ohne eine Verringerung des hohen Sicherheitsstandards in Kauf nehmen zu müssen.

Diese Aufgabe wird durch den kennzeichnenden Teil des Hauptanspruches gelöst.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen näher aufgeführt.

Ein Vorteil der Erfindung besteht darin, daß nach dem erfindungsgemäßen Verfahren vorpersonalisierte Chipkarten bei Antragstellung eines zukünftigen Benutzers diese Karten dezentral in einer ungeschützten Umgebung selbstpersonalisiert und sofort an diesen Benutzer ausgegeben werden können und somit gegenüber dem Verfahren gemäß dem Stand der Technik unumgängliche Wartezeiten entfallen.

Nebenbei kann vorteilhaft eine bereits vorhandene Infrastruktur, wie z. B. Bankfilialen, Postämter usw. bei der Abwicklung des Verfahrens gemäß der Erfindung voll einbezogen werden.

Weiterhin ist von Vorteil, daß bei dem endgültigen Personalisierungsvorgang keine geheimen Daten die Chipkarte verlassen, genausowenig geheime oder sensible Daten in die Karte geschrieben werden.

Beispiele der Erfindung werden anhand der Zeichnung näher erläutert.

Es zeigt die **Fig.** 1 den Stand der Technik der Personalisierung, die **Fig.** 2 das Grundprinzip der Vorpersonalisierung, die **Fig.** 3 die Vorpersonalisierung mit einem zusätzlichen symmetrischen Transportschlüssel und die **Fig.** 4 die endgültige Personalisierung (Selbstpersonalisierung) einer Chipkarte.

Wie **Fig.** 1 zeigt, werden nach der individuellen Erzeugung eines symmetrischen Schlüssels K und nach dem Eingang der Identitätsdaten eines am Chipkartenverfahren zukünftig teilnehmenden Kunden dessen individueller Schlüssel K und der Name der Teilnehmer (Kunden) A in eine freie Chipkarte **2** beim Personalisierungsvorgang eingeschrieben. Gleichzeitig wird in einem Register **3** der Name des Teilnehmers A als Zugangsberechtigung abgelegt.

Diese Vorgänge finden zentral in einem gesicherten Bereich **1** statt. Erst nach der vollständigen und endgültigen Personalisierung kann die Chipkarte **2** diesen gesicherten Bereich **1** verlassen und der Versand der Karte an den Teilnehmer erfolgen.

Von diesem Stand der Technik unterscheidet sich das erfindungsgemäße, in **Fig.** 2 prinzipiell gezeigte Verfahren der Vorpersonalisierung dadurch, daß die Identitätsdaten des zukünftigen Teilnehmers noch nicht bekannt sind und stattdessen eine Pseudo-Identität X erzeugt wird, die mit dem zugehörigen Schlüssel K in die Chipkarte **2** eingeschrieben wird. Diese Pseudo-Identität X wird in einem Register **3** abgelegt. Nach dieser Vorpersonalisierung kann die Chipkarte **2** den gesicherten Bereich **1** verlassen und in Bankfilialen oder Postämter bevorratet werden.

Beantragt ein zukünftiger Teilnehmer eine Chipkarte, so wird in der Filiale oder dem Amt als Selbstpersonalisierer die Pseudo-Identität X mit dem Namen des Teilnehmers A überschrieben und dieser Teilnehmername über eine gesicherte Kommunikationsverbindung zum gesicherten Bereich **1** in dem Register **3** der Pseudo-Identität X eindeutig zugeordnet.

Die **Fig.** 3 zeigt den Vorgang der Vorpersonalisierung unter Verwendung eines zusätzlichen symmetrischen Transportschlüssels t der mit dem individuellen (symmetrischen) Schlüssel K und der Pseudo-Identität X innerhalb des gesicherten Bereichs **1** in die Chipkarte **2** eingegeben wird.

Dieser Transportschlüssel t wird für die gesicherte Kommunikation während des Selbstpersonalisierungsvorgangs zwischen der Kartenausgabestelle und dem gesicherten Bereich (in **Fig.** 2) benötigt.

Die in **Fig.** 4 gezeigte Selbstpersonalisierung in der Kartenausgabestelle läuft in folgenden Schritten ab: Der Teilnehmer gibt seinen Namen A über ein Terminal **5** ein. Eine berechtigte Person, wie z. B. ein Bankangestellter oder ein Postbeamter als Personalisierer leitet den Selbstpersonalisierungsvorgang durch die Eingabe seiner eigenen Berechtigungskarte **4** ein. Diese Berechtigungskarte **4** berechnet anschließend aus dem Namen des Teilnehmers A, der in der Berechtigungskarte **4** abgespeicherten Kennung pi und den ebenfalls abgespeicherten Namen Pi des Personalisierers eine Berechtigungskennung pi(A, Pi), die an die vorpersonalisierte Chipkarte **2** mit dem zusätzlich eingegebenen Namen des Personalisierers Pi weitergeleitet wird.

Innerhalb der Chipkarte **2** wird aus dem Namen des Personalisierers Pi, dem Namen des Teilnehmers A, der Pseudo-Identität X, der aktuellen Zeit h, und der Berechtigungskennung pi (A, Pi) mittels des Transportschlüssels t eine erste Datenfolge t(Pi, A, X, h, pi(A, Pi)) errechnet, die dem gesicherten Bereich **1** übermittelt wird.

Im gesicherten Bereich **1** sind der Transportschlüssel t, der Name der Personalisierers Pi, die Kennung des Personalisierers pi und die Pseudo-Identität X der Chipkarte **2** bekannt. Somit kann aus dieser ersten Datenfolge der Name des Teilnehmers A und zusätzlich zum Vergleich mit den hier bekannten Daten der Name des Personalisierers Pi und die Pseudo-Identität X errechnet werden. Durch einen weiteren Rechenvorgang wird auch die Berechtigungskennung pi(A, Pi) neu erzeugt und überprüft. Sind die Prüfungsergebnisse positiv, so wird mittels des Transportschlüssels t aus der Berechtigungskennung pi(A, Pi) und der Pseudo-Identität X eine zweite Datenfolge t(pi(A, Pi), X) erzeugt und als Bestätigung dem Terminal **5** der Kartenausgabestelle und somit auch der dort befindlichen Chipkarte **2** übermittelt.

Gleichzeitig wird in dem Register der Name des Teilnehmers A der Pseudo-Identität X fest zugeordnet.

Innerhalb der Chipkarte **2** wird abermals die Berechtigungskennung pi(A, Pi) errechnet und mit der dort noch gespeicherten Kennung verglichen. Ist dieser Prüfungsvorgang abgeschlossen, so tauscht die Chipkarte die Pseudo-Identität X mit dem Namen des Teilnehmers A und löscht den Transportschlüssel t und die Berechtigungskennung pi(A, Pi). In der Chipkarte **2** sind also nach der erfolgten Selbstpersonalisierung nur noch der

Name des Teilnehmers A und der zugehörige individuelle Schlüssel K abgespeichert und die Karte kann dem Teilnehmer ausgehändigt werden.

Vorzugsweise ist die Berechtigungskennung pi(A, Pi) eine Einwegfunktion, welche die geheime Kennung pi des Personalisierers beinhaltet. Der Name des Personalisiers Pi kann auch als Codewort in der Berechtigungskarte 4 abgespeichert und/oder in die Chipkarte eingegeben werden.

Wird statt eines symmetrischen Chiffrierverfahrens mit einem individuellen Schlüssel ein asymmetrisches Verfahren gewählt, bei dem ein geheimer und ein öffentlicher Schlüssel als komplementäres Paar verwendet wird, so werden bereits bei der Vorpersonalisierung beide Schlüssel in die Chipkarte abgespeichert und während oder nach der Selbstpersonalisierung nicht gelöscht. Ansonsten unterscheidet sich diese Variante nicht von dem Verfahren mit einem symmetrischen Schlüssel.

Patentansprüche

1. Verfahren zum Personalisieren von Chipkarten bei dem der Name des Teilnehmers und ein zugehöriger individueller Schlüssel in die Chipkarte abgespeichert werden und der Name des Teilnehmers in ein Register abgelegt wird, **dadurch gekennzeichnet,** daß in einem gesicherten Bereich (1) die Chipkarte (2) statt mit dem Namen des Teilnehmers (A) mit einer Pseudo-Indentität (X) vorpersonalisiert wird und diese Pseudo-Indentität (X) in dem Register (3) abgelegt wird und daß erst nach Verlassen der Chipkarte (2) des gesicherten Bereichs (1) in einer Kartenausgabestelle zur Selbstpersonalisierung die Pseudo-Identität (X) mit dem Namen des Teilnehmers (A) überschrieben wird und daß dieser Name über eine gesicherte Kommunikationsverbindung zum gesicherten Bereich (1) der Pseudo-Identität im Register (3) fest zugeordnet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß während der Vorpersonalisierung zusätzlich ein Transportschlüssel (t) für die Kommunikationsverbindung in die Chipkarte (2) eingegeben wird und daß dieser Transportschlüssel (t) nach der Selbstpersonalisierung gelöscht wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß mittels einer Berechtigungskarte (4) eines zugelassenen Personalisierers in der Kartenausgabestelle aus dem Transportschlüssel (t), dem Namen des Personalisierers (Pi), dem Namen des Teilnehmers (A), der Pseudo-Identität (X), der aktuellen Zeit (h) und einer, aus einer geheimen Kennung des Personalisierers (pi), dem Namen des Teilnehmers (A) und dem Namen des Personalisierers (Pi) errechneten Berechtigungskennung (pi(A, Pi)) eine erste Datenfolge als Kommunikationsverbindung errechnet wird, aus der im gesicherten Bereich (1) der Name des Teilnehmers (A) rückgerechnet wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß aus dem Transportschlüssel (t), der Berechtigungskennung (pi(Pi, A) und der Pseudo-Identität (X) innerhalb des gesicherten Bereichs (1) eine zweite Datenfolge errechnet wird und als Teil der Kommunikationsverbindung der Kartenausgabestelle zugeht und dort der Überprüfung der gesamten Kommunikationsverbindung auf Übertragungsfehler dient.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der individuelle Schlüssel (K) ein asymmetricher Schlüssel, bestehend aus einem geheimen und einem öffentlichen Schlüssel ist.

Hierzu 4 Seite(n) Zeichnungen

— Leerseite —

Nummer: DE 39 27 270 A1
Int. Cl.[5]: G 07 C 9/00
Offenlegungstag: 28. Februar 1991

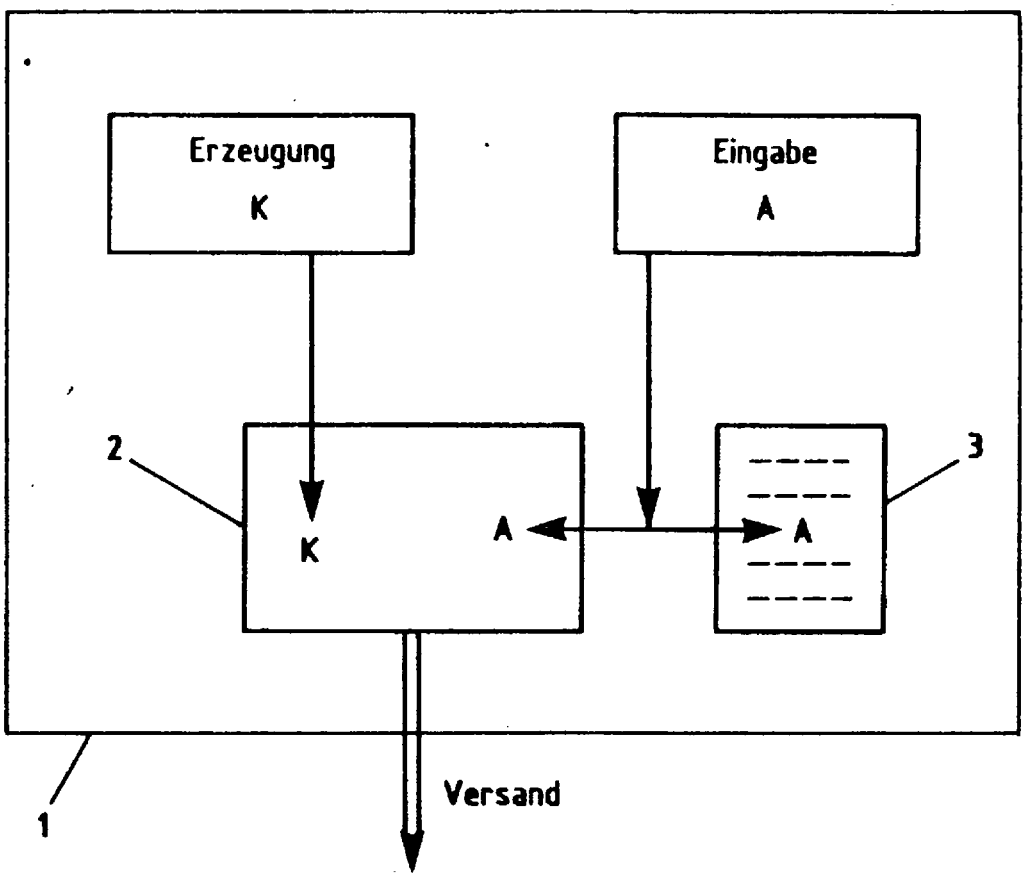

Fig. 1

Nummer: DE 39 27 270 A1
Int. Cl.[5]: G 07 C 9/00
Offenlegungstag: 28. Februar 1991

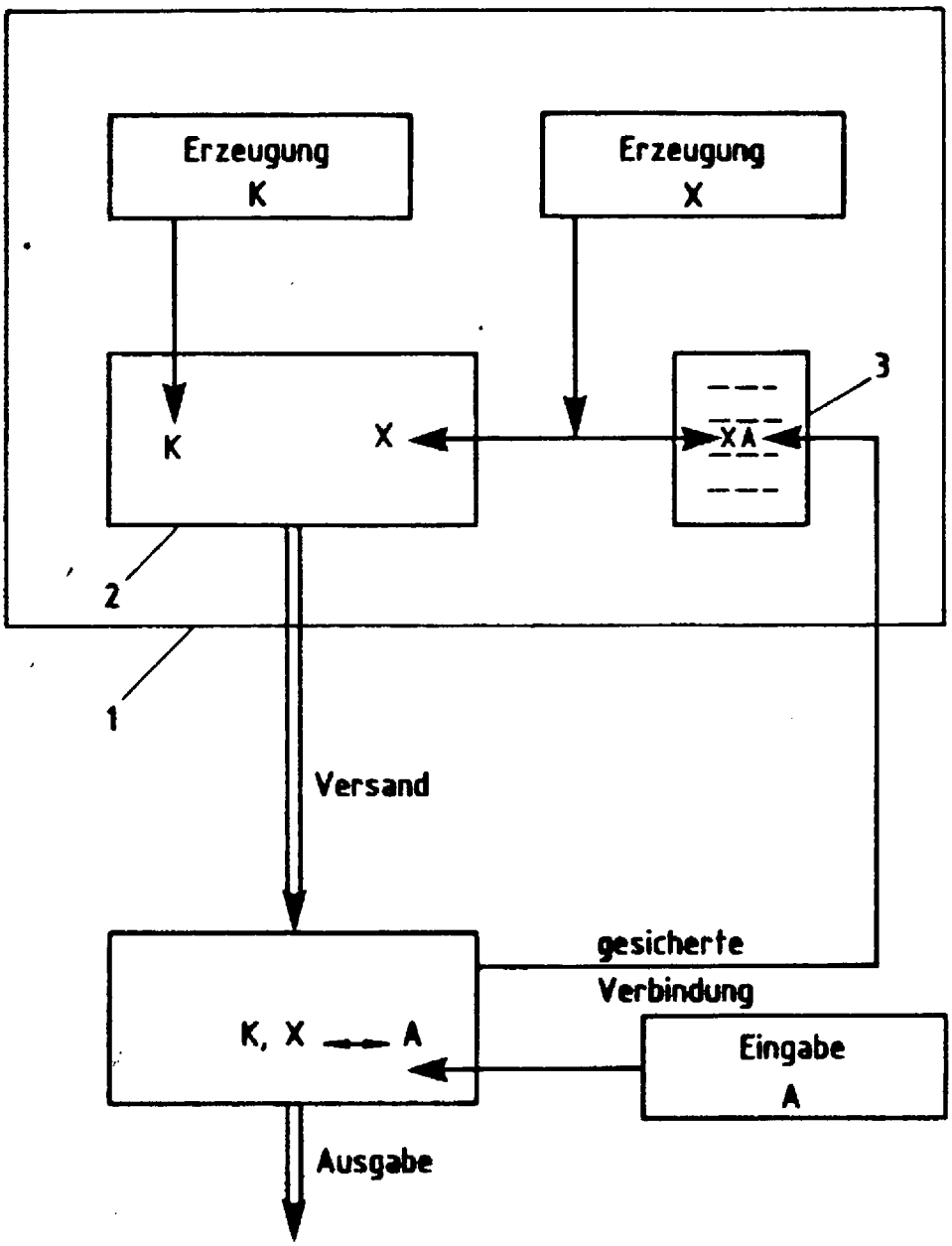

Fig. 2

Nummer: DE 39 27 270 A1
Int. Cl.[5]: G 07 C 9/00
Offenlegungstag: 28. Februar 1991

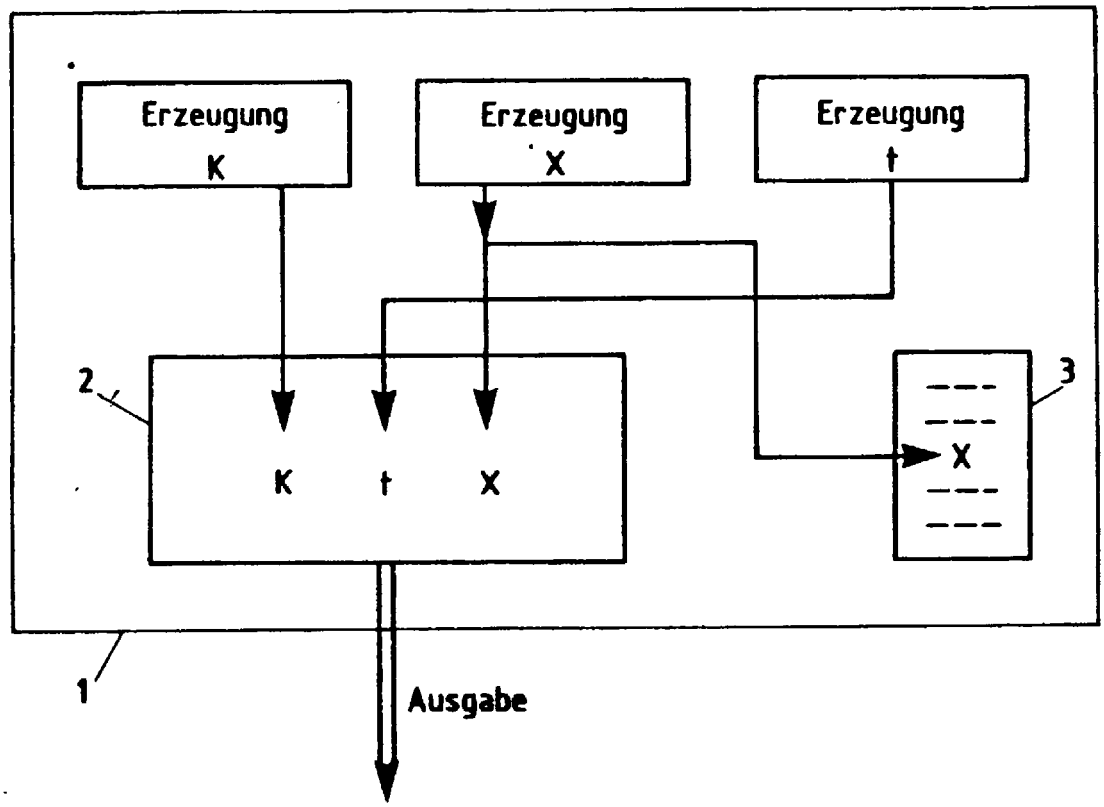

Fig. 3

Nummer: DE 39 27 270 A1
Int. Cl.[5]: G 07 C 9/00
Offenlegungstag: 28. Februar 1991

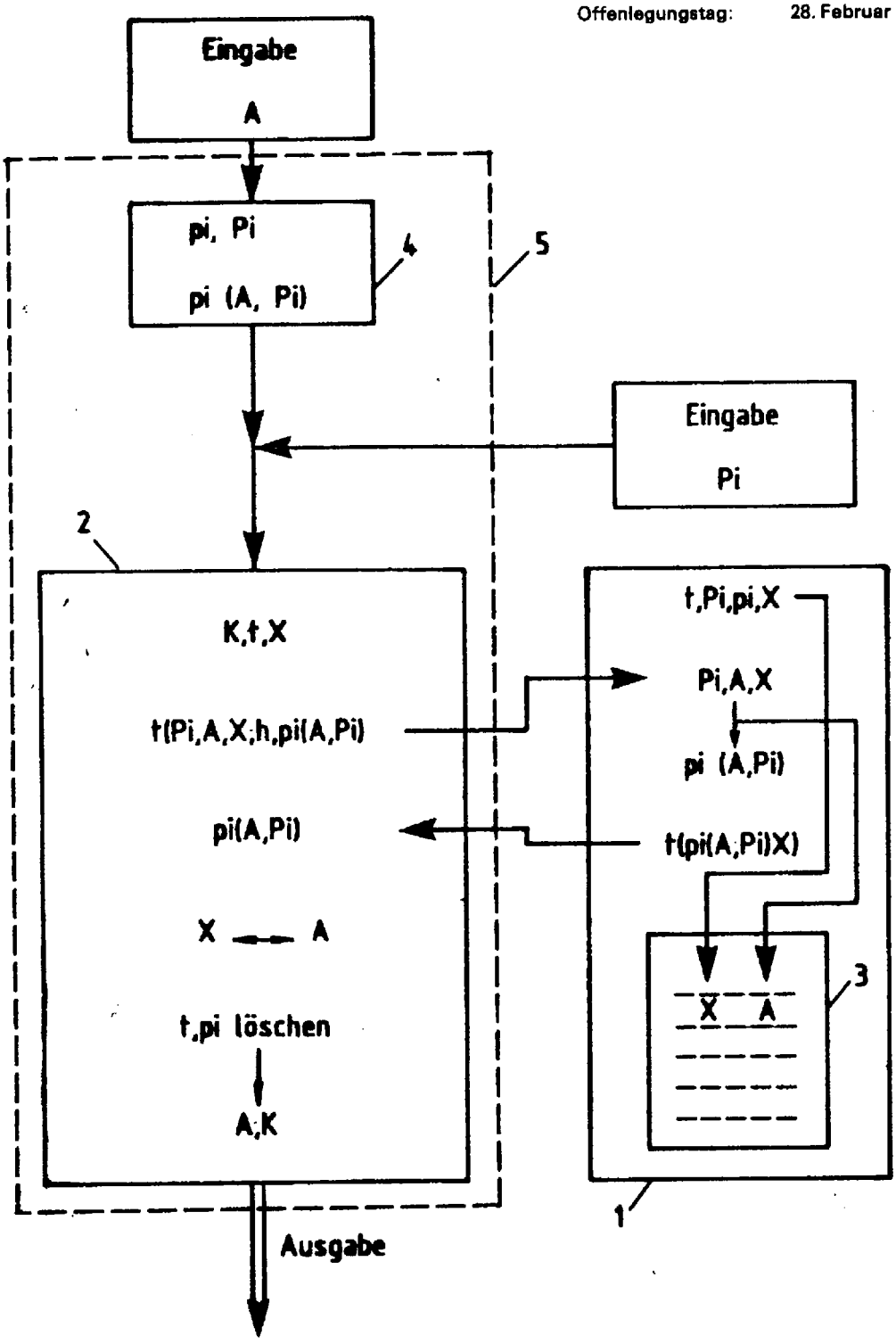

Fig. 4